Discrete Mathematics 309 (2009) 570–575

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the dimensions of the binary codes of a class of unitals

Ka Hin Leung [a], Qing Xiang [b,*]

[a] Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Singapore

[b] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, United States

ARTICLE INFO

Article history:
Received 14 December 2006
Accepted 6 August 2008
Available online 10 September 2008

Keywords:
Buekenhout-Metz unital
Code
Design
Hermitian unital
Ideal
Unital

ABSTRACT

Let U_β be the special Buekenhout-Metz unital in $\mathrm{PG}(2, q^2)$, formed by a union of q conics, where $q = p^e$ is an odd prime power. It can be shown that the dimension of the binary code of the corresponding unital design $\mathcal{U}_\beta$ is less than or equal to $q^3 + 1 - q$. Baker and Wantz conjectured that equality holds. We prove that the aforementioned dimension is greater than or equal to $q^3(1 - \frac{1}{p}) + \frac{q^2}{p}$.

1. Introduction

A *unital* is a 2-$(m^3 + 1, m + 1, 1)$ design, where $m \geq 2$. All known unitals with parameters $(m^3 + 1, m + 1, 1)$ have m equal to a prime power, except for one example with $m = 6$ constructed by Mathon [9], and independently by Bagchi and Bagchi [3]. In this note, we will only consider unitals embedded in $\mathrm{PG}(2, q^2)$, i.e., unitals coming from a set of $q^3 + 1$ points of $\mathrm{PG}(2, q^2)$ which meets every line of $\mathrm{PG}(2, q^2)$ in either 1 or $q + 1$ points. (Sometimes, a point set of size $q^3 + 1$ of $\mathrm{PG}(2, q^2)$ with the above line intersection properties is called a unital, too.) A classical example of such unitals is *the Hermitian unital* $\mathcal{U} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ and $\mathcal{B}$ are the set of absolute points and the set of non-absolute lines of a unitary polarity of $\mathrm{PG}(2, q^2)$, respectively.

The Hermitian unital is a special example of a large class of unitals embedded in $\mathrm{PG}(2, q^2)$, called the *Buekenhout-Metz unitals*. We refer the reader to [5] for a survey of results on these unitals. A subclass of the Buekenhout-Metz unitals which received some attention can be defined as follows.

Let $q = p^e$ be an **odd** prime power, where $e \geq 1$, let β be a primitive element of $\mathbb{F}_{q^2}$, and for $r \in \mathbb{F}_q$ let $C_r = \{(1, y, \beta y^2 + r) \mid y \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 1)\}$. We define

$$U_\beta = \bigcup_{r \in \mathbb{F}_q} C_r.$$

Note that each C_r is a conic in $\mathrm{PG}(2, q^2)$, and any two distinct C_r have only the point $P_\infty = (0, 0, 1)$ in common. Hence $|U_\beta| = q^3 + 1$. It can be shown that every line of $\mathrm{PG}(2, q^2)$ meets U_β in either 1 or $q + 1$ points (see [1,7]). One immediately obtains a unital (design) $\mathcal{U}_\beta$ from U_β: The *points* of $\mathcal{U}_\beta$ are the points of U_β, and the *blocks* of $\mathcal{U}_\beta$ are the intersections of the secant lines with U_β. In this note, we are interested in the binary code $\mathcal{C}_2(\mathcal{U}_\beta)$ of this design, i.e., the $\mathbb{F}_2$-subspace spanned by the characteristic vectors of the blocks of $\mathcal{U}_\beta$ in $\mathbb{F}_2^{U_\beta}$.

* Corresponding author.
E-mail addresses: matlkh@nus.edu.sg (K.H. Leung), xiang@math.udel.edu (Q. Xiang).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.08.004

The following proposition and its proof are due to Baker and Wantz [6,10]. To state the proposition, we use v^S to denote the characteristic vector of a subset S in U_β.

Proposition 1.1 (*Baker and Wantz*). *The vectors v^{C_r}, $r \in \mathbb{F}_q$, form a linearly independent set of vectors in $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$.*

Proof. A binary vector v lies in $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$, if and only if, each block of the design $\mathcal{U}_\beta$ meets the support of v in an even number of points. If a block of $\mathcal{U}_\beta$ goes through P_∞, then it meets every C_r in two points; if a block of $\mathcal{U}_\beta$ does not go through P_∞, then it meets every C_r in either 0 or 2 points. Hence $v^{C_r} \in \mathcal{C}_2(\mathcal{U}_\beta)^\perp$, for every $r \in \mathbb{F}_q$. The q conics C_r have only the point P_∞ in common. Thus, v^{C_r}, $r \in \mathbb{F}_q$, are linearly independent. The proof is complete. □

An immediate corollary of Proposition 1.1 is that $\dim \mathcal{C}_2(\mathcal{U}_\beta)^\perp \geq q$. Hence $\dim \mathcal{C}_2(\mathcal{U}_\beta) \leq q^3 + 1 - q$. Baker and Wantz [6,10] made the following conjecture.

Conjecture 1.2 (*Baker and Wantz*). *The 2-rank of $\mathcal{U}_\beta$ is $q^3 + 1 - q$. That is, $\dim \mathcal{C}_2(\mathcal{U}_\beta) = q^3 + 1 - q$.*

Wantz [10] verified Conjecture 1.2 in the cases where $q = 3, 5, 7$, and 9 by using a computer and MAGMA [4]. Gary Ebert [6] popularized the above conjecture of Baker and Wantz in a talk in Oberwolfach in 2001. See also [11] for a description of the above conjecture. Of course, the conjecture is equivalent to saying that $\dim \mathcal{C}_2(\mathcal{U}_\beta)^\perp = q$. So it suffices to show that $\{v^{C_r} \mid r \in \mathbb{F}_q\}$ spans $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$. That is, we need to show that if $S \subset U_\beta$ and S meets every block of $\mathcal{U}_\beta$ in an even number of points, then S is a union of some C_r's, or a union of some C_r's with P_∞ deleted. We have not been able to prove this equivalent version of the conjecture. What we could prove is a lower bound on $\dim \mathcal{C}_2(\mathcal{U}_\beta)$ as stated in the abstract. The main idea in our proofs is to realize a shortened code of $\mathcal{C}_2(\mathcal{U}_\beta)$ as an ideal in a certain group algebra of the elementary abelian p-group of order q^3. We hope that the current note will stimulate further research on this conjecture.

2. A lower bound on the dimension of $\mathcal{C}_2(\mathcal{U}_\beta)$

We first consider the automorphisms of $\mathcal{U}_\beta$. Let

$$G = \{\theta \in \mathrm{PGL}(3, q^2) \mid \theta(U_\beta) = U_\beta\}$$

be the linear collineation group of $\mathrm{PG}(2, q^2)$ fixing U_β as a set. It was shown by Baker and Ebert [2] that

$$G = T \rtimes \mathbb{Z}_{2(q-1)},$$

where T is an elementary abelian group of order q^3, and $\mathbb{Z}_{2(q-1)}$ is a cyclic group of order $2(q-1)$. The group G certainly is also an automorphism group of the design $\mathcal{U}_\beta$ since any element of G maps a secant line of U_β to a secant line of U_β. In fact, the group T above acts regularly on $U_\beta \setminus \{P_\infty\}$. Explicitly,

$$T = \left\{ \begin{pmatrix} 1 & t & \beta t^2 \\ 0 & 1 & 2\beta t \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, t \in \mathbb{F}_{q^2}, r \in \mathbb{F}_q \right\} \cong (\mathbb{F}_{q^2}, +) \times (\mathbb{F}_q, +).$$

In the rest of the paper, we will use $T(t, r)$, $t \in \mathbb{F}_{q^2}$, $r \in \mathbb{F}_q$, to denote the element

$$\begin{pmatrix} 1 & t & \beta t^2 \\ 0 & 1 & 2\beta t \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

of T.

The coordinates of the code $\mathcal{C}_2(\mathcal{U}_\beta)$ are labeled by the points in U_β. Deleting the coordinate labeled by P_∞ from all codewords of $\mathcal{C}_2(\mathcal{U}_\beta)$, we get a shortened (or punctured) code $\mathcal{C}_2(\mathcal{U}_\beta)'$, which has the same dimension over $\mathbb{F}_2$ as $\mathcal{C}_2(\mathcal{U}_\beta)$ since $v^{\{P_\infty\}} \notin \mathcal{C}_2(\mathcal{U}_\beta)$. Since T acts regularly on $U_\beta \setminus \{P_\infty\}$, we may identify the coordinates of $\mathcal{C}_2(\mathcal{U}_\beta)'$ with the elements of T. Under this identification, the point $(1, t, \beta t^2 + r)$ of U_β correspond to the group element $T(t, r)$ since

$$(1, 0, 0) \cdot T(t, r) = (1, t, \beta t^2 + r).$$

After the above identification, the code $\mathcal{C}_2(\mathcal{U}_\beta)'$ becomes an ideal of the group algebra $\mathbb{F}_2[T]$. Now we can use the characters of T to help compute the dimension of $\mathcal{C}_2(\mathcal{U}_\beta)'$.

First of all, we need to extend the field over which the code $\mathcal{C}_2(\mathcal{U}_\beta)$ is defined. Let $K = \mathbb{F}_{2^m}$, where $m = \mathrm{ord}_p(2)$ is the order of 2 modulo p (i.e., m is the smallest positive integer such that $2^m \equiv 1 \pmod p$). So K contains a primitive pth root of unity ξ_p. We consider the code $\mathcal{C}_K(\mathcal{U}_\beta)$ and puncture it at P_∞ to get $\mathcal{C}_K(\mathcal{U}_\beta)'$, which will be denoted by M for simplicity of notation. The code M is an ideal of the group algebra $K[T]$, and

$$\dim_K(M) = \dim_{\mathbb{F}_2}(\mathcal{C}_2(\mathcal{U}_\beta)').$$

Therefore, Conjecture 1.2 is equivalent to the statement that

$$\dim_K(M) = q^3 + 1 - q.$$

Since M is an ideal of $K[T]$, and T is abelian, it is well known [8, p. 277] that

$$\dim_K(M) = |\{\chi \in \hat{T} \mid Me_\chi \neq 0\}|,$$

where $\hat{T}$ is the group of characters $\chi : T \to K^*$ of T, and

$$e_\chi = \frac{1}{|T|} \sum_{g \in T} \chi(g^{-1}) g$$

are primitive idempotents of $K[T]$. We also mention that for any $h \in T$ and any $\chi \in \hat{T}$,

$$h \cdot e_\chi = \chi(h) e_\chi. \tag{2.1}$$

Since $T \cong (\mathbb{F}_{q^2}, +) \times (\mathbb{F}_q, +)$, every character χ of T can be written as $(\psi_a, \lambda_b) : T \to K^*$, where $a \in \mathbb{F}_{q^2}$, $b \in \mathbb{F}_q$,

$$\psi_a : x \mapsto \xi_p^{\mathrm{Tr}_{q^2/p}(ax)}, \quad x \in \mathbb{F}_{q^2},$$

and

$$\lambda_b : y \mapsto \xi_p^{\mathrm{Tr}_{q/p}(by)}, \quad y \in \mathbb{F}_q.$$

Here $\mathrm{Tr}_{q^2/p}$ (resp. $\mathrm{Tr}_{q/p}$) is the trace from $\mathbb{F}_{q^2}$ (resp. $\mathbb{F}_q$) to $\mathbb{F}_p$. (We note in passing that $\mathrm{Tr}_{q^2/p}(a/2) = \mathrm{Tr}_{q/p}(a)$ for all $a \in \mathbb{F}_q$, a fact which will be used in the proof of Theorem 2.4.) Hence we need to count the number of pairs $(a, b) \in \mathbb{F}_{q^2} \times \mathbb{F}_q$ such that

$$Me_{(\psi_a, \lambda_b)} \neq 0.$$

To this end, we need to write down the blocks of the unital design $\mathcal{U}_\beta$ more explicitly.

We first recall some properties of U_β, which will be used to describe the blocks of $\mathcal{U}_\beta$. The proofs of these properties can be found in [1,2,7].

- Among the $q^2 + 1$ lines through P_∞, q^2 of them are secant to U_β, and one is tangent to U_β. The secant lines through P_∞ are $[t, 1, 0]$, where $t \in \mathbb{F}_{q^2}$, and the unique tangent line through P_∞ is $[1, 0, 0]$.
- A secant line to U_β, not through P_∞ must pass through $(0, 1, \alpha)$ for some $\alpha \in \mathbb{F}_{q^2}$. Moreover, for every $\alpha \in \mathbb{F}_{q^2}$, there are $q^2 - q$ secant line through $(0, 1, \alpha)$.
- The line $[t, -\alpha, 1]$, $t, \alpha \in \mathbb{F}_{q^2}$, through $(0, 1, \alpha)$ is secant to U_β if and only if $t \notin \mathbb{F}_q + \frac{\alpha^2}{4\beta}$. (This can be seen as follows: The line $[t, -\alpha, 1]$ is tangent to U_β if and only if it is tangent to some conic C_r, $r \in \mathbb{F}_q$, which in turn is equivalent to $\alpha^2 - 4\beta(t + r) = 0$. The last condition is simply saying that $t \in \mathbb{F}_q + \frac{\alpha^2}{4\beta}$.)

The unital design $\mathcal{U}_\beta$ has a total of $q^2(q^2 - q + 1)$ blocks, which fall into two types. The type I blocks are the intersections of the q^2 secant lines through P_∞ with U_β. These are

$$U_\beta \cap [t, 1, 0] = \{(1, -t, \beta t^2 + r) \mid r \in \mathbb{F}_q\} \cup \{P_\infty\},$$

where $t \in \mathbb{F}_{q^2}$. We may identify $(U_\beta \cap [t, 1, 0]) \setminus \{P_\infty\}$ with the group ring element

$$B_{t,\infty} := \sum_{r \in \mathbb{F}_q} T(-t, r) \in K[T]. \tag{2.2}$$

The type II blocks are the intersections of the secant lines through $(0, 1, \alpha)$ with U_β, with $q^2 - q$ of them for each $\alpha \in \mathbb{F}_{q^2}$. These blocks are

$$U_\beta \cap [t, -\alpha, 1] = \{(1, y, \beta y^2 + r) \mid r \in \mathbb{F}_q, y \in \mathbb{F}_{q^2}, t - \alpha y + \beta y^2 + r = 0\},$$

where $\alpha \in \mathbb{F}_{q^2}$ and $t \in \mathbb{F}_{q^2} \setminus (\mathbb{F}_q + \frac{\alpha^2}{4\beta})$. We may identify the above block with the group ring element

$$B_{t,\alpha} := \sum_{y \in \mathbb{F}_{q^2}, r = -t + \alpha y - \beta y^2 \in \mathbb{F}_q} T(y, r) \in K[T]. \tag{2.3}$$

Therefore we have a complete description of the blocks of the unital design $\mathcal{U}_\beta$.

Lemma 2.1. *With the above notation, $Me_{(\psi_a, \lambda_0)} \neq 0$, for all $a \in \mathbb{F}_{q^2}$.*

Proof. We will show that $B_{t,\infty} \cdot e_{(\psi_a,\lambda_0)} \neq 0$, where $B_{t,\infty}$ is defined in (2.2). By (2.1), we have $h \cdot e_\chi = \chi(h)e_\chi$ for any $h \in T$ and any $\chi \in \hat{T}$. So we need to show that $(\psi_a, \lambda_0)(B_{t,\infty}) \neq 0$.

$$\begin{aligned}(\psi_a, \lambda_0)(B_{t,\infty}) &= \sum_{r\in\mathbb{F}_q} \psi_a(-t)\lambda_0(r)\\ &= \sum_{r\in\mathbb{F}_q} \psi_a(-t)\\ &= q \cdot \psi_a(-t).\end{aligned}$$

Since q is odd, and $\psi_a(-t)$ is a root of unity in K, we see that $(\psi_a, \lambda_0)(B_{t,\infty}) \neq 0$. The proof is complete. □

Lemma 2.2. *With the above notation, $Me_{(\psi_0,\lambda_b)} = 0$, for all nonzero $b \in \mathbb{F}_q$.*

Proof. The ideal M is generated by two types of elements $B_{t,\infty}$ and $B_{t,\alpha}$, which correspond to the two types of blocks of $\mathcal{U}_\beta$. We will show that the character (ψ_0, λ_b), $b \neq 0$, is zero on both types of generating elements.

For any type I element $B_{t,\infty}$, $t \in \mathbb{F}_{q^2}$, in (2.2), we have

$$\begin{aligned}(\psi_0, \lambda_b)(B_{t,\infty}) &= \sum_{r\in\mathbb{F}_q} \psi_0(-t)\lambda_b(r)\\ &= \sum_{r\in\mathbb{F}_q} \lambda_b(r)\\ &= 0,\end{aligned}$$

since b is nonzero.

For any type II element $B_{t,\alpha}$ in (2.3), we have

$$\begin{aligned}(\psi_0, \lambda_b)(B_{t,\alpha}) &= \sum_{r\in\mathbb{F}_q, y\in\mathbb{F}_{q^2}, r=-(\beta y^2-\alpha y+t)} \psi_0(y)\lambda_b(r)\\ &= \sum_{r\in\mathbb{F}_q, y\in\mathbb{F}_{q^2}, r=-(\beta y^2-\alpha y+t)} \lambda_b(r)\\ &= 0,\end{aligned}$$

since two distinct $y \in \mathbb{F}_{q^2}$ give rise to the same $r \in \mathbb{F}_q$. The proof is complete. □

By the above two lemmas, we see that Conjecture 1.2 is equivalent to

Conjecture 2.3. *For nonzero $a \in \mathbb{F}_{q^2}$ and nonzero $b \in \mathbb{F}_q$, one has*

$$Me_{(\psi_a,\lambda_b)} \neq 0.$$

Up to now we have only been able to prove some partial results on this latter conjecture.

Theorem 2.4. *Let $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_q^*$. If $\mathrm{Tr}_{q^2/p}(\frac{a^2}{2b\beta}) \neq 0$, then $Me_{(\psi_a,\lambda_b)} \neq 0$.*

Proof. Let $t, \alpha \in \mathbb{F}_{q^2}$ with $\Delta := t - \frac{\alpha^2}{4\beta} \notin \mathbb{F}_q$. Then $[t, -\alpha, 1]$ is a secant line to U_β, and

$$U_\beta \cap [t, -\alpha, 1] = \{(1, y, \beta y^2 + r) \mid y \in \mathbb{F}_{q^2}, r = -t + \alpha y - \beta y^2 \in \mathbb{F}_q\}.$$

This set can be identified with the group ring element

$$B_{t,\alpha} = \sum_{y\in A_{t,\alpha}} T(y, -t + \alpha y - \beta y^2) \in K[T],$$

where $A_{t,\alpha} = \{y \in \mathbb{F}_{q^2} \mid t - \alpha y + \beta y^2 \in \mathbb{F}_q\}$.

Now let $\mu \in \mathbb{F}_{q^2}^*$ such that $\mu^2 \in \mathbb{F}_q^*$ (explicitly, $\mu \in \langle \beta^{\frac{q+1}{2}} \rangle$, the subgroup of order $2(q-1)$ of $\mathbb{F}_{q^2}^*$). Then $[t\mu^2, -\alpha\mu, 1]$ is also a secant line to U_β, and

$$U_\beta \cap [t\mu^2, -\alpha\mu, 1] = \{(1, z, \beta z^2 + r) \mid z \in \mathbb{F}_{q^2}, r = -t\mu^2 + \alpha\mu z - \beta z^2 \in \mathbb{F}_q\}.$$

This set can be identified with the group ring element

$$B_{t\mu^2,\alpha\mu} = \sum_{y\in A_{t,\alpha}} T(\mu y, -\mu^2(t - \alpha y + \beta y^2)) \in K[T].$$

Since $\Delta \notin \mathbb{F}_q$, the set $(\mathbb{F}_q - \Delta)$ contains $\frac{q+1}{2}$ nonsquares of $\mathbb{F}_{q^2}$, say $n_1, n_2, \ldots, n_{\frac{q+1}{2}}$ (see Lemma 5.2 in [7]). Now we can write down the elements of $A_{t,\alpha}$ explicitly. Note that $t - \alpha y + \beta y^2 \in \mathbb{F}_q$, if and only if, $\beta(y - \frac{\alpha}{2\beta})^2 \in \mathbb{F}_q - \Delta$, which in turn is equivalent to $\beta(y - \frac{\alpha}{2\beta})^2 = n_i$ for some i, $1 \le i \le (q+1)/2$. Therefore, we have $y \in A_{t,\alpha}$ if and only if $y = \frac{\alpha}{2\beta} \pm \sqrt{\beta^{-1} n_i}$, $1 \le i \le (q+1)/2$. It follows that

$$B_{t\mu^2,\alpha\mu} = \sum_{i=1}^{\frac{q+1}{2}} T\left(\frac{\alpha\mu}{2\beta} \pm \sqrt{\beta^{-1} n_i \mu^2}, -\mu^2(n_i + \Delta)\right).$$

Now

$$\begin{aligned}(\psi_a, \lambda_b)(B_{t\mu^2,\alpha\mu}) &= \sum_{i=1}^{\frac{q+1}{2}} \left(\xi_p^{\mathrm{Tr}_{q^2/p}(\frac{\alpha\mu}{2\beta} + a\sqrt{\beta^{-1} n_i \mu^2})} + \xi_p^{\mathrm{Tr}_{q^2/p}(\frac{\alpha\mu}{2\beta} - a\sqrt{\beta^{-1} n_i \mu^2})}\right) \xi_p^{\mathrm{Tr}_{q/p}(-b\mu^2(n_i+\Delta))} \\ &= \xi_p^{\mathrm{Tr}_{q^2/p}(\frac{a\alpha\mu}{2\beta} - \frac{b\Delta\mu^2}{2})} \sum_{i=1}^{\frac{q+1}{2}} \left(\xi_p^{\mathrm{Tr}_{q^2/p}(a\sqrt{\beta^{-1} n_i \mu^2})} + \xi_p^{\mathrm{Tr}_{q^2/p}(-a\sqrt{\beta^{-1} n_i \mu^2})}\right) \xi_p^{\mathrm{Tr}_{q^2/p}(-\frac{b n_i \mu^2}{2})}.\end{aligned}$$

Define

$$S_{t\mu^2,-\alpha\mu} := \sum_{i=1}^{\frac{q+1}{2}} \left(\xi_p^{\mathrm{Tr}_{q^2/p}(a\sqrt{\beta^{-1} n_i \mu^2})} + \xi_p^{\mathrm{Tr}_{q^2/p}(-a\sqrt{\beta^{-1} n_i \mu^2})}\right) \xi_p^{\mathrm{Tr}_{q^2/p}(-\frac{b n_i \mu^2}{2})}.$$

Let R be a complete set of coset representatives of the subgroup $\{1, -1\}$ in $\langle \beta^{\frac{q+1}{2}} \rangle$ (so $|R| = (q-1)$). We will show that

$$\sum_{\mu \in R} S_{t\mu^2,-\alpha\mu} \neq 0. \tag{2.4}$$

From (2.3), we immediately see that there exists some $\mu \in R$ such that $(\psi_a, \lambda_b)(B_{t\mu^2,\alpha\mu}) \neq 0$, which proves the conclusion of the theorem.

First we claim that as μ runs through R and i runs through $1, 2, \ldots, \frac{q+1}{2}$, $n_i\mu^2$ run through the set N of nonsquares of $\mathbb{F}_{q^2}^*$. The claim can be proved as follows. Clearly, each $n_i\mu^2$ is a nonsquare of $\mathbb{F}_{q^2}^*$. It suffices to show that $n_i\mu^2$, $1 \le i \le \frac{q+1}{2}$ and $\mu \in R$, are all distinct. Assume that $n_i\mu^2 = n_j\lambda^2$, for some $1 \le i, j \le \frac{q+1}{2}$, and some $\mu, \lambda \in R$. Since $n_i, n_j \in \mathbb{F}_q - \Delta$, we set $n_i = x - \Delta$ and $n_j = y - \Delta$, where $x, y \in \mathbb{F}_q$. We have

$$\mu^2 x - \mu^2 \Delta = \lambda^2 y - \lambda^2 \Delta.$$

Noting that $\mu^2, \lambda^2 \in \mathbb{F}_q$ and $\Delta \notin \mathbb{F}_q$, we see that $\mu^2 = \lambda^2$. Since $\mu, \lambda \in R$, we must have $\mu = \lambda$, from which we deduce $n_i = n_j$. The claim is proved.

For convenience, we will use S to denote the set of nonzero squares of $\mathbb{F}_{q^2}$. So we have

$$\begin{aligned}\sum_{\mu \in R} S_{t\mu^2,-\alpha\mu} &= \sum_{x \in N} \left(\xi_p^{\mathrm{Tr}_{q^2/p}(a\sqrt{\beta^{-1}x})} + \xi_p^{\mathrm{Tr}_{q^2/p}(-a\sqrt{\beta^{-1}x})}\right) \xi_p^{\mathrm{Tr}_{q^2/p}(-\frac{bx}{2})} \\ &= \sum_{y \in S} \left(\xi_p^{\mathrm{Tr}_{q^2/p}(a\sqrt{y})} + \xi_p^{\mathrm{Tr}_{q^2/p}(-a\sqrt{y})}\right) \xi_p^{\mathrm{Tr}_{q^2/p}(\frac{-b\beta y}{2})} \\ &= \sum_{z \in \mathbb{F}_{q^2}^*} \xi_p^{\mathrm{Tr}_{q^2/p}(az - \frac{b\beta z^2}{2})} \\ &= \sum_{z \in \mathbb{F}_{q^2}} \xi_p^{\mathrm{Tr}_{q^2/p}(az - \frac{b\beta z^2}{2})} - 1 \\ &= \xi_p^{\mathrm{Tr}_{q^2/p}(\frac{a^2}{2b\beta})} \sum_{x \in \mathbb{F}_{q^2}} \xi_p^{\mathrm{Tr}_{q^2/p}(-\frac{b\beta}{2}x^2)} - 1.\end{aligned}$$

Note that p is odd and $\mathrm{Tr}_{q^2/p}(-\frac{b\beta}{2}x^2) = \mathrm{Tr}_{q^2/p}(-\frac{b\beta}{2}(-x)^2)$ for any $x \in \mathbb{F}_{q^2}$. As $\xi_p \in K$ and K has characteristic 2, we have

$$\sum_{x \in \mathbb{F}_{q^2}} \xi_p^{\mathrm{Tr}_{q^2/p}(-\frac{b\beta}{2}x^2)} = 1.$$

Hence

$$\sum_{\mu\in R} S_{t\mu^2,-\alpha\mu} = \xi_p^{\mathrm{Tr}_{q^2/p}(\frac{a^2}{2b\beta})} - 1.$$

Therefore, if $\mathrm{Tr}_{q^2/p}(\frac{a^2}{2b\beta}) \neq 0$, then $\sum_{\mu\in R} S_{t\mu^2,-\alpha\mu} \neq 0$. The proof is complete. □

An immediate corollary is the following.

Corollary 2.5. $\dim C_2(\mathcal{U}_\beta) \geq q^3(1-\frac{1}{p}) + \frac{q^2}{p}$.

Proof. By Lemma 2.1, we have q^2 characters (ψ_a, λ_0), $a \in \mathbb{F}_{q^2}$, of T such that $Me_{(\psi_a,\lambda_0)} \neq 0$.

Next, for each $b \in \mathbb{F}_q^*$, the number of a's such that $\mathrm{Tr}_{q^2/p}(\frac{a^2}{2b\beta}) \neq 0$ is $(q^2 - p^{2e-1}) = (q^2 - q^2/p)$. So Theorem 2.4 produces $(q-1)(q^2 - q^2/p)$ characters (ψ_a, λ_b) of T, such that $Me_{(\psi_a,\lambda_b)} \neq 0$.

Therefore, $\dim C_2(\mathcal{U}_\beta) \geq q^2 + (q-1)(q^2 - q^2/p) = q^3(1-\frac{1}{p}) + \frac{q^2}{p}$. The proof is complete. □

Acknowledgements

The work in this paper was done during a visit of the second author to the National University of Singapore (NUS) in 2003. The second author thanks the Department of Mathematics of NUS for its hospitality. We also would like to thank Gary Ebert and Peter Sin for many helpful discussions. Last but not the least we thank two anonymous referees for their careful reading of the paper and constructive suggestions.

References

[1] R.D. Baker, G.L. Ebert, Intersection of unitals in the Desarguesian plane, Cong. Numer. 70 (1990) 87–94.
[2] R.D. Baker, G.L. Ebert, On Buekenhout-Metz unitals of odd order, J. Combin. Theory (A) 60 (1992) 67–84.
[3] S. Bagchi, B. Bagchi, Designs from pairs of finite fields: I A cyclic unital $U(6)$ and other regular Steiner 2-designs, J. Combin. Theory (A) 52 (1989) 51–61.
[4] J. Cannon, C. Playoust, An Introduction to MAGMA, University of Sydney, Sydney, Australia, 1993.
[5] G.L. Ebert, Buekenhout unitals, Combinatorics (Assisi, 1996), Discrete Math. 208–209 (1999) 247–260.
[6] G.L. Ebert, Binary codes of odd order Buekenhout-Metz unitals, talk given in Oberwolfach, Dec. 2001.
[7] J.W.P. Hirschfeld, T. Szönyi, Sets in a finite plane with few intersection numbers and a distinguished point, Discrete Math. 97 (1991) 229–242.
[8] E.S. Lander, Symmetric Designs: An Algebraic Approach, in: London Mathematical Society Lecture Note Series, vol. 74, Cambridge University Press, Cambridge, 1983.
[9] R. Mathon, Constructions of cyclic 2-designs, Ann. Disc. Math. 34 (1987) 353–362.
[10] K. Wantz, Personal communication, Jan. 2004.
[11] Q. Xiang, Recent results on p-ranks and Smith normal forms of some 2-(v, k, λ) designs, in: Coding Theory and Quantum Computing, in: Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 53–67.